Electronic Version
Stylesheet Version v1.1.1

Claims

[c1] 1. A method for controlling connections to a computer upon its initial deployment, the method comprising:
upon initial deployment of the computer, applying a preconfigured security policy that establishes a restricted zone of preapproved hosts that the computer may connect to upon its initial deployment;
receiving a request for a connection from the computer to a particular host;
based on said preconfigured security policy, determining whether the particular host is within the restricted zone of preapproved hosts; and
blocking said connection if said particular host is not within the restricted zone of preapproved hosts.

[c2] 2. The method of claim 1, further comprising:
prior to initial deployment of the computer, imaging a hard disk of the computer with said preconfigured security policy.

[c3] 3. The method of claim 1, wherein the computer comprises a portable computer and initial deployment includes establishing Internet connectivity.

[c4] 4. The method of claim 1, wherein the restricted zone comprises a pre-access restricted zone specifically for a new machine.

[c5] 5. The method of claim 1, wherein said preconfigured security policy operates to prevent the computer from being remotely accessed by another computer upon initial deployment.

[c6] 6. The method of claim 1, wherein said preconfigured security policy operates to prevent the computer from being remotely probed for vulnerabilities by other computers.

[c7] 7. The method of claim 1, wherein said preconfigured security policy operates to prevent the computer from being infected by a malicious program delivered through an open port.

[c8] 8. The method of claim 1, wherein said blocking step includes:
instructing a firewall, which is responsive to said preconfigured security policy, to block connections to any host that is not within the restricted zone of preapproved hosts.

[c9] 9. The method of claim 1, wherein the preapproved hosts comprise specific security-relevant sites.

[c10] 10. The method of claim 9, wherein specific security-relevant sites include antivirus Web sites.

[c11] 11. The method of claim 9, wherein specific security-relevant sites include firewall Web sites.

[c12] 12. The method of claim 9, wherein specific security-relevant sites include end point security Web sites.

[c13] 13. The method of claim 1, wherein other attempted connections to the computer are refused.

[c14] 14. The method of claim 1, further comprising:
upon the computer completing updating of security sub-systems, removing the restricted zone so that the computer may connect to other machines.

[c15] 15. The method of claim 14, wherein the restricted zone is removed by replacing the preconfigured security policy with an updated security policy.

[c16] 16. The method of claim 1, wherein the preconfigured security policy is preinstalled on the computer prior to user purchase.

[c17] 17. The method of claim 1, wherein the computer includes a hard disk having a manufacturer-provided disk image, and wherein the manufacturer-provided disk im-

age includes the preconfigured security policy.

[c18] 18. The method of claim 1, wherein the computer is not allowed to participate with general connectivity to the Internet until security-relevant updates have been performed.

[c19] 19. The method of claim 18, further comprising:
providing an option that allows a user to override the preconfigured security policy.

[c20] 20. The method of claim 19, further comprising:
providing a warning to any user that overrides the preconfigured security policy.

[c21] 21. The method of claim 19, further comprising:
displaying a disclaimer to any user that overrides the preconfigured security policy that indicates that the user assumes responsibility.

[c22] 22. The method of claim 9, wherein specific security-relevant sites include operating system-related Web sites.

[c23] 23. The method of claim 1, further comprising:
upon a first attempted connection of the computer, downloading an updated list of hosts that the computer may initially connect to.

[c24] 24. A computer-readable medium having processor-executable instructions for performing the method of claim 1.

[c25] 25. A downloadable set of processor-executable instructions for performing the method of claim 1.

[c26] 26. A computer system that is preconfigured to control connections upon initial deployment, the system comprising:
a computer having a preconfigured security policy that establishes a restricted zone of preapproved hosts that the computer may connect to upon initial deployment of the computer;
a connectivity module for processing user requests for the computer to connect to a particular host; and
a security module for determining whether the particular host is within the restricted zone of preapproved hosts based on said preconfigured security policy, and for blocking any attempt to connect to a host that is not within the restricted zone of preapproved hosts.

[c27] 27. The system of claim 26, further comprising:
a hard disk that receives a hard disk image having said preconfigured security policy.

[c28] 28. The system of claim 26, wherein the computer com-

prises a portable computer and initial deployment includes establishing Internet connectivity.

[c29] 29. The system of claim 26, wherein the restricted zone comprises a pre-access restricted zone specifically for a new machine.

[c30] 30. The system of claim 26, wherein said preconfigured security policy operates to prevent the computer from being remotely accessed by another computer upon initial deployment.

[c31] 31. The system of claim 26, wherein said preconfigured security policy operates to prevent the computer from being remotely probed for vulnerabilities by other computers.

[c32] 32. The system of claim 26, wherein said preconfigured security policy operates to prevent the computer from being infected by a malicious program delivered through an open port.

[c33] 33. The system of claim 26, wherein the security module blocks attempts by instructing a firewall, which is responsive to said preconfigured security policy, to block connections to any host that is not within the restricted zone of preapproved hosts.

[c34] 34. The system of claim 26, wherein the preapproved hosts comprise specific security-relevant sites.

[c35] 35. The system of claim 34, wherein specific security-relevant sites include antivirus Web sites.

[c36] 36. The system of claim 34, wherein specific security-relevant sites include firewall Web sites.

[c37] 37. The system of claim 34, wherein specific security-relevant sites include end point security Web sites.

[c38] 38. The system of claim 26, wherein other attempted connections to the computer are refused.

[c39] 39. The system of claim 26, further comprising:
a module for removing the restricted zone so that the computer may connect to other machines.

[c40] 40. The system of claim 39, wherein the restricted zone is removed by replacing the preconfigured security policy with an updated security policy.

[c41] 41. The system of claim 26, wherein the preconfigured security policy is preinstalled on the computer prior to user purchase.

[c42] 42. The system of claim 26, wherein the computer includes a hard disk having a manufacturer-provided disk

image, and wherein the manufacturer-provided disk image includes said preconfigured security policy.

[c43] 43. The system of claim 26, wherein the computer is not allowed to participate with general connectivity to the Internet until security-relevant updates have been performed.

[c44] 44. The system of claim 43, wherein the security module includes an option that allows a user to override the preconfigured security policy.

[c45] 45. The system of claim 44, wherein the security module displays a warning to any user that overrides the preconfigured security policy.

[c46] 46. The system of claim 44, wherein the security module displays a disclaimer to any user that overrides the preconfigured security policy that indicates that the user assumes responsibility.

[c47] 47. The system of claim 34, wherein specific security-relevant sites include operating system-related Web sites.

[c48] 48. The system of claim 26, wherein the security module downloads an updated list of hosts that the computer may initially connect to.

[c49] 49. A method for enforcing pre-access connectivity restrictions on a new machine, the method comprising:
detecting attempts to connect the new machine to other devices;
determining, based on an initial security policy that establishes a restricted zone of acceptable connections, which devices the new machine is permitted to connect to; and
blocking any connection that attempts to connect the new machine to a device outside the restricted zone of acceptable connections.

[c50] 50. The method of claim 49, further comprising:
prior to initial deployment of the new machine, imaging a hard disk of the new machine with said initial security policy.

[c51] 51. The method of claim 49, wherein the new machine comprises a portable computer and initial deployment includes establishing Internet connectivity.

[c52] 52. The method of claim 49, wherein said restricted zone comprises a pre-access restricted zone specifically for a new machine.

[c53] 53. The method of claim 49, wherein said initial security policy operates to prevent the new machine from being

remotely accessed by another computer upon initial deployment.

[c54] 54. The method of claim 49, wherein said initial security policy operates to prevent the new machine from being remotely probed for vulnerabilities by other computers.

[c55] 55. The method of claim 49, wherein said initial security policy operates to prevent the new machine from being infected by a malicious program delivered through an open port.

[c56] 56. The method of claim 49, wherein said blocking step includes:
instructing a firewall, which is responsive to said initial security policy, to block connections to any host that is not within the restricted zone of preapproved hosts.

[c57] 57. The method of claim 56, wherein the preapproved hosts comprise specific security-relevant sites.

[c58] 58. The method of claim 57, wherein specific security-relevant sites include antivirus Web sites.

[c59] 59. The method of claim 57, wherein specific security-relevant sites include firewall Web sites.

[c60] 60. The method of claim 57, wherein specific security-relevant sites include end point security Web sites.

[c61] 61. The method of claim 49, wherein other attempted connections to the new machine are refused.

[c62] 62. The method of claim 49, further comprising:
upon the new machine completing updating of security subsystems, removing the restricted zone so that the new machine may connect to other machines.

[c63] 63. The method of claim 62, wherein the restricted zone is removed by replacing the initial security policy with an updated security policy.

[c64] 64. The method of claim 49, wherein the initial security policy is preinstalled on the new machine prior to user purchase.

[c65] 65. The method of claim 49, wherein the new machine includes a hard disk having a manufacturer-provided disk image, and wherein the manufacturer-provided disk image includes said initial security policy.

[c66] 66. The method of claim 49, wherein the new machine is not allowed to participate with general connectivity to the Internet until security-relevant updates have been completed.

[c67] 67. The method of claim 66, further comprising:
providing an option that allows a user to override the

initial security policy.

[c68] 68. The method of claim 67, further comprising: providing a warning to any user that overrides the initial security policy.

[c69] 69. The method of claim 67, further comprising: displaying a disclaimer to any user that overrides the initial security policy that indicates that the user assumes responsibility.

[c70] 70. The method of claim 57, wherein specific security-relevant sites include operating system-related Web sites.